BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
Emily A. Horne (State Bar No. 347723)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
ehorne@bursor.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

BARTON GOLUB, individually and on behalf of all other persons similarly situated,

Plaintiff,

v.

THEHUFFINGTONPOST.COM, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

PAGE

NATURE OF THE ACTION 1
THE PARTIES 2
JURISDICTION AND VENUE 2
FACTUAL ALLEGATIONS 3
I. THE CALIFORNIA INVASION OF PRIVACY ACT 3
II. DEFENANT VIOLATES THE CIPA 5
A. The Mechanics Of IP Addresses 5
1. Differentiating Between A Public Versus Private IP Address 6
2. Privacy Implications of Public IP Addresses 9
B. The Trackers Are "Pen Registers" 12
1. Connatix Tracker 13
2. ADNXS Tracker 15
3. OpenX Tracker 18
III. DEFENDANT'S CONDUCT CONSTITUTES AN INVASION OF PLAINTIFF'S AND CLASS MEMBERS' PRIVACY 20
A. Data Brokers and Real-Time Bidding: The Information Economy 21
1. Data Brokers 21
2. Real-Time Bidding 25
B. Defendant Uses The Connatix Tracker For Targeted Advertising And Data Monetization 29
C. Defendant Uses The ADNXS Tracker For Targeted Advertising And Data Monetization 31
D. Defendant Uses The OpenX Tracker For Identity Resolution, Targeted Advertising, And Data Monetization 33
IV. PLAINTIFF'S EXPERIENCE 36
CLASS ALLEGATIONS 37
CAUSES OF ACTION 39
PRAYER FOR RELIEF 40
JURY DEMAND 40

Plaintiff Barton Golub ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his attorneys, makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself and his counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. Defendant TheHuffingtonPost.com, Inc., ("Defendant" or "The Huffington Post") owns and operates https://huffpost.com (the "Website").

2. When users visit the Website, Defendant causes three Trackers—the Connatix Tracker, ADNXS Tracker, and OpenX Tracker (collectively, the "Trackers")—to be installed on Website visitors' internet browsers. The Trackers are operated by separate and distinct third parties: Connatix, Microsoft, and OpenX, respectively (the "Third Parties'). Through these Trackers, each of the Third Parties collect Website users' internet protocol ("IP") addresses and other device identifier information such as device type, browser type, and unique and persistent identifiers ("Device Fingerprints"). Defendant and these Third Parties then uses the data collected by the Trackers for hyper-targeted marketing and advertising.

3. Because the Trackers capture Website visitors' "routing, addressing, or signaling information," the Trackers constitute a "pen register" under Section 638.50(b) of the California Invasion of Privacy Act ("CIPA"). Cal. Penal Code § 638.50(b).

4. By installing and using the Trackers without Plaintiff's prior consent and without a court order, Defendant violated CIPA § 638.51(a).

5. The allegations here are made more invasive by the entities operating the Trackers and collecting Plaintiff's and Class Members' IP Addresses and Device Fingerprints. OpenX is a data broker that adds the IP addresses and Device Fingerprints to comprehensive user profiles and uses that information to track Plaintiff and Class Members across the Internet. OpenX also crosschecks the IP addresses and Device Fingerprints against any profiles in its possession to identify Website users. Those data profiles are then provided to advertisers for more targeted and tailored advertising based on a broad universe of information. Microsoft and Connatix facilitate that targeted

advertising by using IP addresses and Device Fingerprints to allow advertisers to target specific users or groups of users with specific advertisements based on that information. All of this enriches Defendant, who is able to monetize its Website as the beneficiary of that advertising revenue. Indeed, Defendant is able to increase the value of its user base to prospective advertisers by allowing OpenX to connect IP addresses and Device Fingerprints to broader profiles of other personal information.

6. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of California residents, and to recover statutory damages for Defendant's violation of CIPA § 638.51.

THE PARTIES

7. Plaintiff Golub resides in San Francisco, California and has an intent to remain there, and is therefore a citizen of California. Plaintiff Golub was in California when he visited the Website.

8. Defendant TheHuffingtonPost.com, Inc. is a Delaware corporation with its principal place of business in New York, New York.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(a) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00 exclusive of interest and costs, there are over 100 members of the putative class, and at least one class member is a citizen of a different state than Defendant.

10. This Court has jurisdiction over Defendant because Defendant purposefully availed itself of this forum by conducting substantial business within California such that Defendant has significant, continuous, and pervasion contacts with the State of California.

11. Specifically, through Defendant's installation and use of the Trackers on the Website, Defendant is able to engage in "programmatic advertising," which is the process of "buy[ing] and sell[ing] digital ads. Programmatic advertising serves up relevant ad impressions to audiences

through automated steps, in less than a second."[1] The Third Parties are each players in the programmatic advertising space.

12. By using the Trackers, Defendant is able to target users with advertisements relevant to not only who they are, but where they are located. That is, California Website users will see different advertisements than New York Website users based (in part) on location, as ascertained from IP addresses. Thus, Defendant purposefully availed itself of the California market because it caused the Third Parties to collect the IP addresses and Device Fingerprints of Californians, used this information in conjunction with the Third Parties to target Californians with advertisements relevant to their location, and reaped substantial revenue from this unlawful disclosure of Website users' information. Defendant did this knowingly, as users are identified based on OpenX's technology and Defendant is able to (and does) target advertising campaigns at California specifically.

13. This Court is the proper venue for this action pursuant to 28 U.S.C. § 1391 because a substantial part of the events giving rise to Plaintiff's claims took place within this District.

FACTUAL ALLEGATIONS

I. THE CALIFORNIA INVASION OF PRIVACY ACT

14. The California Legislature enacted CIPA to protect certain privacy rights of California citizens. The California Legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

15. As relevant here, CIPA section 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

16. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

[1] WHAT IS PROGRAMMATIC ADVERTISING?, https://advertising.amazon.com/blog/programmatic-advertising.

17. A "trap and trace device" is a "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(b).

18. In plain English, a "pen register" is a "device or process" that records *outgoing* information, while a "trap and trace device" is a "device or process" that records *incoming* information.

19. Historically, law enforcement used "pen registers" to record the numbers of outgoing calls from a particular telephone line, while law enforcement used "trap and trace devices" to record the numbers of incoming calls to that particular telephone line. As technology advanced, however, courts have expanded the application of these surveillance devices.

20. For example, if a user sends an email, a "pen register" might record the email address it was sent from, the email address the email was sent to, and the subject line—because this is the user's *outgoing* information. On the other hand, if that same user receives an email, a "trap and trace device" might record the email address it was sent from, the email address it was sent to, and the subject line—because this is *incoming* information that is being sent to that same user.

21. Although CIPA was enacted before the dawn of the Internet, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc.* 2013 WL 5423918, at *21 (N.D. Cal. Sep. 26, 2013); *see also, e.g.*, *Shah v. Fandom, Inc*, --- F. Supp. 3d ---, 2024 WL 4539577, at *21 (N.D. Cal. Oct. 21, 2024) (finding trackers similar to those at issue here were "pen registers" and noting "California courts do not read California statutes as limiting themselves to the traditional technologies or models in place at the time the statutes were enacted"); *Mirmalek v. Los Angeles Times Communications LLC*, 2024 WL 5102709, at *3-4 (N.D. Cal. Dec. 12, 2024) (same); *Moody v. C2 Educ. Sys. Inc.* --- F. Supp. 3d ---, 2024 WL 3561367, at *3 (C.D. Cal. July 25, 2024) ("Plaintiff's allegations that the TikTok Software is embedded in the Website and collects information from visitors plausibly fall within the scope of §§ 638.50 and 638.51.");*Greenley v. Kochava, Inc*, 684 F. Supp. 3d 1024,

1050 (S.D. Cal. 2023) (referencing CIPA's "expansive language" when finding software was a "pen register"); *Javier v. Assurance IQ, LLC,* 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, [CIPA] Section 631(a) applies to Internet communications."). This accords with the fact that, "when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc.*, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

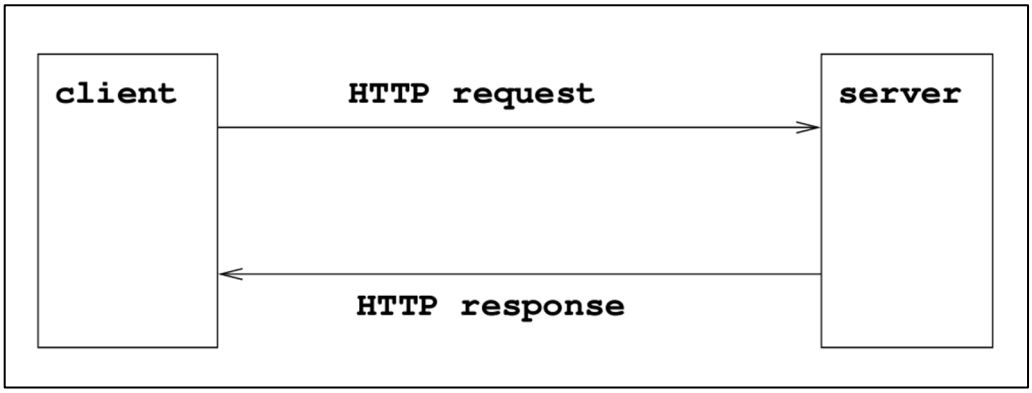
22. Individuals may bring an action against the violator of any provision of CIPA—including CIPA § 638.51—for $5,000 per violation. Cal. Penal Code § 637.2(a)(1).

II. DEFENANT VIOLATES THE CIPA

A. The Mechanics Of IP Addresses

23. To make Defendant's Website load on a user's internet browser, the browser sends an "HTTP request" or "GET" request to Defendant's server where the relevant Website data is stored. In response to the request, Defendant's server sends an "HTTP response" back to the browser with a set of instructions. A general diagram of this process is pictured at Figure 1, which explains how Defendant's Website transmits instructions back to users' browsers in response to HTTP requests. *See* Figure 1.

Figure 1:



24. The server's instructions include how to properly display the Website—*e.g.*, what images to load, what text should appear, or what music should play.

25. In addition, the server's instructions cause the Trackers to be installed on a user's browser. The Trackers then cause the browser to send identifying information—including the user's

IP address and Device Fingerprints—to Microsoft, Connatix, and OpenX. The Third Parties' Trackers will also set a user ID unique to their Tracker that also allows the user to be tracked across the Internet.

26. An IP address is a unique identifier for a device, which is expressed as four sets of numbers separated by periods (*e.g.*, 192.168.123.132). The traditional format of IP addresses is called IPv4, and it has a finite amount of combinations and thus is limited to approximately 4.3 billion addresses. Because this proved to be insufficient as the Internet grew, IPv6 was introduced. IPv6 offers a vastly larger address space with 340 undecillion possible addresses. While IPv6 adoption has been increasing, many networks still rely on IPv4.[2]

27. Much like a telephone number, an IP address guides or routes an intentional communication signal (*i.e.*, a data packet) from one device to another. An IP address is essential for identifying a device on the internet or within a local network, facilitating smooth communication between devices.

1. Differentiating Between A Public Versus Private IP Address

28. A public IP address is accessible from anywhere on the internet; it is assigned by an Internet Service Provider ("ISP") and it is unique globally. Public IP addresses are required for devices that need direct internet access.

29. While public IP addresses are unique, they are not necessarily "public" in the sense that they are freely accessible. If an individual is not actively sending data packets out, the public IP address remains private and is not broadcast to the wider internet.

30. Public IP addresses can be used to determine the approximate physical location of a device. For example, services like iplocation.io use databases that map IP addresses to geographic areas—often providing information about the country, city, approximate latitude and longitude coordinates, or even the internet service provider associated with the public IP. This geolocation capability is leveraged by online advertising and user identification services.

[2] *See, e.g.*, *What is the Internet Protocol*, CLOUDFLARE, https://www.cloudflare.com/learning/network-layer/internet-protocol/; Stefano Gridelli, *What is an RFC1918 Address?*, NETBEEZ (Jan. 22, 2020), https://netbeez.net/blog/rfc1918/.

31. A private IP address is used within an internal network and is not routable on the public internet. The Internet Assigned Numbers Authority ("IANA") reserves specific ranges of numbers to be exclusively used for private IP addresses (*e.g.*, 172.16.0.0 through 172.31.255.255). Thus, private IP addresses can be used repeatedly across different networks because they are isolated from the global internet. For example, a home network in New York and an office network in Tokyo can both use the same private IP address (*e.g.*, 192.168.1.1) for their routers without conflict.

32. The distinction between a public and private IP address is fundamental to the architecture of modern networks. Public IP addresses facilitate global communication, while private IP addresses conserve the finite amount of combinations to make an IP address through local network communication. And crucially, a private IP address does not divulge a user's geolocation, whereas a public IP address does and is thus extensively used in advertising.

33. An analogy is useful. A public IP address is like the number for a landline telephone for a household. A private IP address is like each handset that is connected to that landline number (*e.g.*, "Handset #1," "Handset #2"). Nothing can be gleaned from knowing Handset #1 versus Handset #2 is making a call. But a lot can be gleaned from knowing the phone number who is making the call.

34. The same is true of IP addresses. Nothing can be gleaned from determining whether a user is using their laptop or smartphone to access a website by itself.[3] But the public IP address divulges the approximate location of the user that is connecting to the Internet and the router directing those communications (presumably the user's house or workplace), and it is the means through which the user actually communicates with the website and the Internet at large.

35. Thus, the differences between public and private IP addresses are as follows:[4]

[3] That being said, as discussed below, the Trackers also collect "device identifier information," which is used alongside the IP address to digitally "fingerprint" individuals. So, by installing the Trackers on Website users' browsers, Defendant allows third parties to collect information that is analogous to a telephone number (the public IP address) and the specific handset that is making the call (the device identifier information).

[4] *What's The Difference Between A Public And Private IP Address?*, AVIRA (Jan. 31, 2024), https://www.avira.com/en/blog/public-vs-private-ip-address.

Figure 2:

Category	Private IP address	Public IP address
Scope	The private IP address only has a local scope in your own network.	The public IP address's scope is global.
Communication	It is used so devices within a network can communicate with each other.	It allows access to the internet and is used for communication outside of your own network.
Uniqueness	It's an address from a smaller range that's used by other devices in other local networks.	It's a unique address that's not used by other devices on the internet.
Provider	The router assigns a private IP address to a specific device on the local network.	The internet service provider assigns the public IP address.
Range	Private IP address ranges: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255	Any IP address that isn't within a private IP address range.

36. A public IP address is therefore "routing, addressing, or signaling information."

37. A public IP address is "addressing" information because it determines the general geographic coordinates of the user who is accessing a website.

38. A public IP address is "routing" or "signaling" information because it is sending or directing the user's communication from the router in their home or work to the website they are communicating with, and ensuring that "emails, websites, streaming content, and other data reaches you correctly"[5]:

//

//

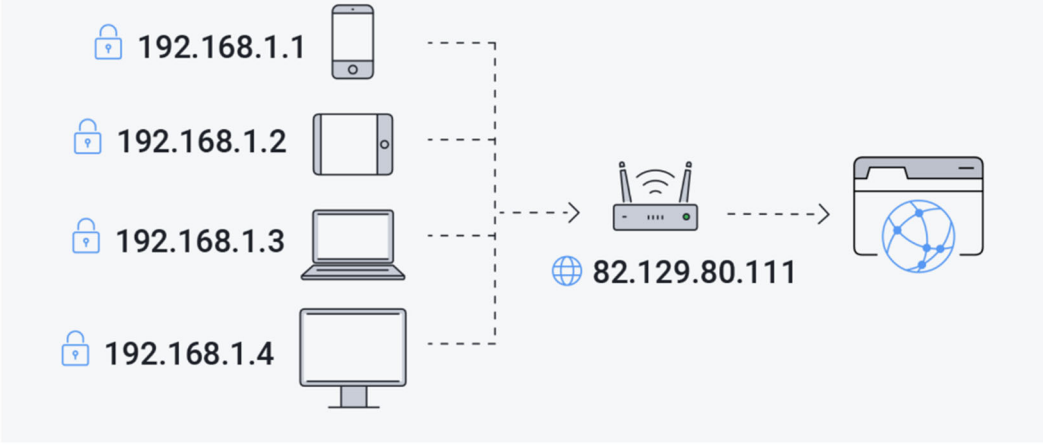
//

//

//

[5] Anthony Freda, *Private IP vs Public IP: What's the Difference?*, AVG (June 4, 2021), https://www.avg.com/en/signal/public-vs-private-ip-address.

Figure 3:



Each device on a network has a private IP address, and the router has a public IP address to communicate with the rest of the internet.

2. Privacy Implications of Public IP Addresses

39. Through a public IP address, a device's state, city, zip code, and approximate latitude and longitude can be determined. Thus, knowing a user's public IP address—and therefore geographical location—"provide[s] a level of specificity previously unfound in marketing."[6]

40. A public IP address allows advertisers to (i) "[t]arget [customers by] countries, cities, neighborhoods, and … postal code"[7] and (ii) "to target specific households, businesses[,] and even individuals with ads that are relevant to their interests."[8] Indeed, "IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service"[9] because "[c]ompanies can use an IP address … to personally identify individuals."[10]

41. In fact, a public IP address is a common identifier used for "geomarketing," which is

[6] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.

[7] *Location-Based Targeting That Puts You in Control*, CHOOZLE, https://choozle.com/geotargeting-strategies/.

[8] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf.

[9] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.

[10] Trey Titone, *The Future Of Ip Address As An Advertising Identifier*, AD TECH EXPLAINED (May 16, 2022), https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/.

"the practice of using location data to identify and serve marketing messages to a highly-targeted audience. Essentially, geomarketing allows [websites] to better serve [their] audience by giving [them] an inside look into where they are, where they have been, and what kinds of products or services will appeal to their needs."[11] For example, for a job fair in specific city, companies can send advertisements to only those in the general location of the upcoming event.[12]

42. "IP targeting is a highly effective digital advertising technique that allows you to deliver ads to specific physical addresses based on their internet protocol (IP) address. IP targeting technology works by matching physical addresses to IP addresses, allowing advertisers to serve ads to specific households or businesses based on their location."[13]

43. "IP targeting capabilities are highly precise, with an accuracy rate of over 95%. This means that advertisers can deliver highly targeted ads to specific households or businesses, rather than relying on more general demographics or behavioral data."[14]

44. In addition to "reach[ing] their target audience with greater precision," businesses are incentivized to use a customer's public IP address because it "can be more cost-effective than other forms of advertising."[15] "By targeting specific households or businesses, businesses can avoid wasting money on ads that are unlikely to be seen by their target audience."[16]

45. In addition, "IP address targeting can help businesses to improve their overall marketing strategy."[17] "By analyzing data on which households or businesses are responding to their

---

[11] *See, e.g.*, *The Essential Guide to Geomarketing: Strategies, Tips & More*, DEEP SYNC (Nov. 20, 2023), https://deepsync.com/geomarketing/.

[12] *See, e.g.*, *Personalize Your Website And Digital Marketing Using IP Address*, GEOFLI, https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns.

[13] *IP Targeting*, SAVANT DSP, https://www.savantdsp.com/ip-targeting?gad_source=1&gclid=Cj0KCQjw1Yy5BhD-ARIsAI0RbXZJKJSqMI6p1xAxyqai1WhAiXRJTbX8qYhNuEvIfSCJ4jfOV5-5maUaAgtNEALw_wcB.

[14] *Id.*

[15] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf.

[16] *Id.*

[17] *Id.*

ads, businesses can refine their targeting strategy and improve their overall marketing efforts."[18]

46. The collection of IP addresses here is particularly invasive here given OpenX's status as a data broker. As a report from NATO found:

> [a] data broker may receive information about a[] [website] user, including his … IP address. The user then opens the [website] while his phone is connected to his home Wi-Fi network. When this happens, the data broker can use the IP address of the home network to identify the user's home, and append this to the unique profile it is compiling about the user. If the user has a computer connected to the same network, this computer will have the same IP address. The data broker can then use the IP address to connect the computer to the same user, and identify that user when their IP address makes requests on other publisher pages within their ad network. Now the data broker knows that the same individual is using both the phone and the computer, which allows it to track behaviour across devices and target the user and their devices with ads on different networks.[19]

47. In other words, not only does the collection of IP addresses by the Third Parties cause harm in and of itself, OpenX specifically attaches IP addresses to comprehensive user profiles, tracking Plaintiff and Class Members across the Internet using their IP addresses and compiling vast reams of other personal information in the process.

48. For these reasons, under Europe's General Data Protection Regulation, IP addresses are considered "personal data, as they can potentially be used to identify an individual."[20]

49. As alleged below, Defendant installs each of the Trackers on the user's browser for marketing and analytics purposes, and the Trackers collect information—users' IP addresses—that identifies the outgoing "routing, addressing, or signaling information" of the user. Accordingly, the Trackers are each "pen registers."

---

[18] *Id.*

[19] HENRIK TWETMAN & GUNDARS BERGMANIS-KORATS, NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, DATA BROKERS AND SECURITY at 11 (2020), https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf.

[20] *Is an IP Address Personal Data?, Convesio*, https://convesio.com/knowledgebase/article/is-an-ip-address-personal-data/; *see also What Is Personal Data?*, EUROPEAN COMMISSION, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en.

B. The Trackers Are "Pen Registers"

50. Defendant owns and operates the Website. The Website is a news site that reports on news, politics, lifestyle, and entertainment.[21] The Website reports on "a diverse range of topics" related to global and local news.[22]

51. When companies build their websites, they install or integrate various third-party scripts into the code of the website in order to collect data from users or perform other functions.[23]

52. Often times, third-party scripts are installed on websites "for advertising purposes."[24]

53. Further, "[i]f the same third-party tracker is present on many sites, it can build a more complete profile of the user over time."[25]

54. Defendant has long incorporated the Trackers' code into the code of its Website, including when Plaintiff and Class Members visited the Website. Thus, when Plaintiff visited the Website, the Website caused the Trackers to be installed on Plaintiff's and other users' browsers.

55. As described below, when a user visits the Website, the Website's code—as programmed by Defendant—installs the Trackers onto the user's browser. This allows the Third Parties—through their respective Trackers—to collect Plaintiff's and Class Members' IP addresses and Device Fingerprints, and pervasively track them across the Internet.

56. The Trackers also causes additional data points to be sent from Plaintiff's and Class Members' browser to the Third Parties, which are meant to uniquely identify users across sessions and devices. In addition to the public IP address, key elements include the user-agent string (browser, operating system, and device type) and device capabilities such as supported image formats and compression methods. Persistent identifiers like the PUID, GUID, UID, PSVID, and User-Agent

---

[21] *About Us*, HUFFPOST, https://www.huffpost.com/static/about-us.

[22] *Id.*

[23] *See Third-party Tracking*, PIWIK, https://piwik.pro/glossary/third-party-tracking/ ("Third-party tracking refers to the practice by which a tracker, other than the website directly visited by the user, traces or assists in tracking the user's visit to the site. Third-party trackers are snippets of code that are present on multiple websites. They collect and send information about a user's browsing history to other companies…").

[24] *Id.*

[25] *Id.*

ensure users can be tracked even after clearing standard session data like cookies. Advanced methods like fingerprinting and server-side matching remain unaffected by cookie deletion. Combined, these elements form a detailed, unique fingerprint that allows for cross-site tracking and behavioral profiling.

57. Defendant and the Third Parties then use the public IP addresses, Device Fingerprints, and other information of Website visitors that are collected and set by the Trackers, including those of Plaintiff and Class Members, to deanonymize Plaintiff and Class Members, serve hyper-targeted advertisements, and unjustly enrich themselves through this improperly collected information.

58. At no time prior to the installation and use of the Trackers on Plaintiff's and Class Members's browsers, or prior to the use of the Trackers, did Defendant procure Plaintiff's and Class Members's consent for such conduct. Nor did Defendant obtain a court order to install or use the Trackers.

1. Connatix Tracker

59. Connatix is a software-as-a-service company that develops and operates the Connatix Tracker, which it provides to website owners like Defendant for a fee. As described in more detail below, Connatix operates an "Advertising Exchange."

60. According to Connatix, it helps "350+ publisher groups across thousands of sites" to "deliver, monetize, analyze and create video, while providing advertisers with premium video inventory and a collection of data intelligence solutions …."[26] Through its products, Connatix offers "a proprietary ad server [and] exchange" that enable its clients, like Defendant, to "[b]oost revenue."[27]

61. In other words, Connatix "collects and processes your personal information" and then "share[s] your personal information for online behaviorally targeted ads,"[28] specifically, video ads.

[26] *Connatix and JW Player Merge to Create the Industry's Largest Video Technology and Monetization Platform*, PR NEWSWIRE (Oct. 9, 2024), https://www.prnewswire.com/news-releases/connatix-and-jw-player-merge-to-create-the-industrys-largest-video-technology-and-monetization-platform-302271377.html?tc=eml_cleartime (last visited Dec. 23, 2024).

[27] *Video Analytics*, CONNATIX, https://connatix.com/video-analytics (last visited Dec. 23, 2024).

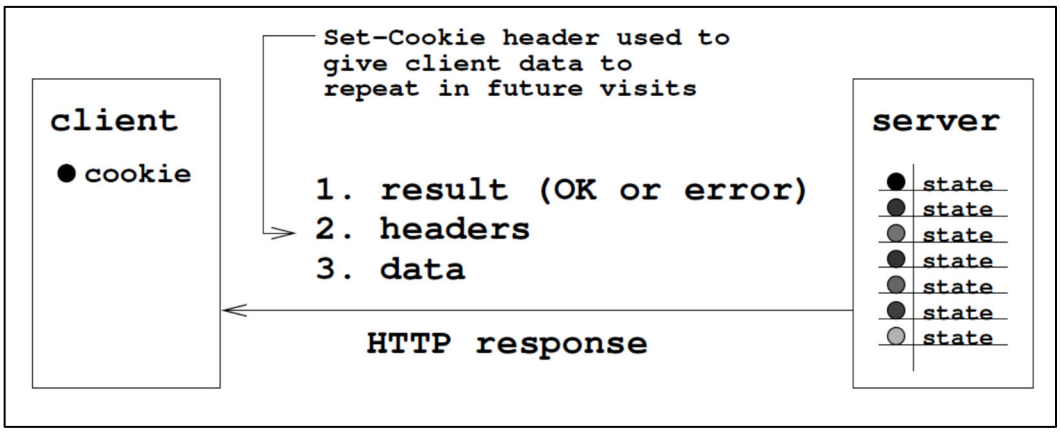
[28] DO NOT SELL OR SHARE MY PERSONAL INFORMATION, CONNATIX, https://connatix.com/optout (last visited Dec. 23, 2024).

To achieve this, Connatix uses its Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Website.

62. The first time a user visits Defendant's Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends an HTTP response with directions to install the Connatix Tracker on the user's browser. The Connatix Tracker, in turn, instructs the user's browser to send Connatix the user's IP address and Device Fingerprints (the "user-agent" string below).

63. Moreover, Connatix stores a cookie (the "cnx_userId" below) with the user's IP address and Device Fingerprints in the user's browser cache. When the user subsequently visits Defendant's Website, the Connatix Tracker locates the cookie identifier stored on the user's browser. If the cookie is stored on the browser, the Connatix Tracker causes the browser to send the cookie along with the user's IP address and Device Fingerprints to Connatix. A general diagram of this process is pictured as Figure 4, which explains how the Website causes the Connatix Tracker to install a cookie on the user's browser and instructs the user's browser to send the user's IP address along with the cookie:

Figure 4:

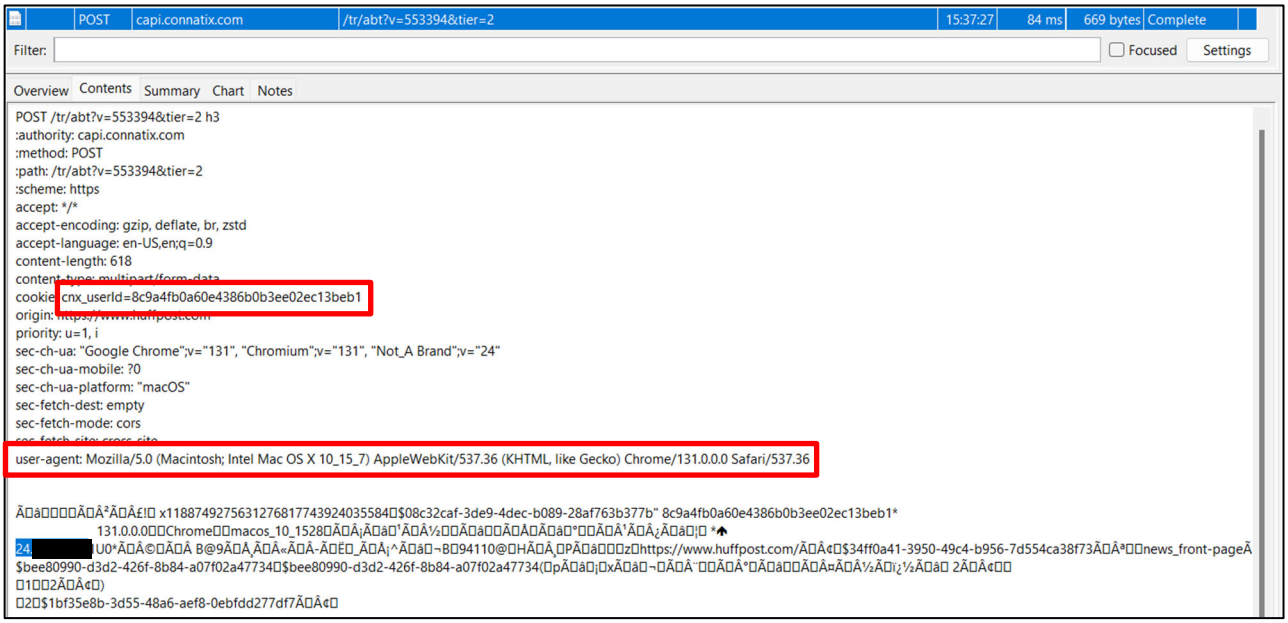


64. If the user clears his or her cookies, then the user wipes out the Connatix Tracker from its cache. Accordingly, the next time the user visits Defendant's Website the process begins over again: (i) Defendant's server installs the Connatix Tracker on the user's browser, (ii) the Connatix Tracker instructs the browser to send Connatix the user's IP address and Device Fingerprints,

(iii) the Connatix Tracker stores a cookie in the browser cache, and (iv) Connatix will continue to receive the user's IP address and Device Fingerprints on subsequent Website visits as part of the cookie transmission.

65. In all cases, however, Connatix receives a user's IP address, Device Fingerprints, and user information every time its Tracker is loaded by Defendant's Website, as the below screenshot from Plaintiff's visit to the Website indicates[29]:

Figure 5:



66. The Connatix Tracker is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, 684 F. Supp. 3d at 1050.

67. Further, the Connatix Tracker is a "device" because "for software to work, it must be run on some kind of computing device." *James v. Walt Disney Co.*, 701 F. Supp. 3d 942, 958 (N.D. Cal. 2023).

68. Because the Connatix Tracker captures the outgoing information—the IP address—from visitors to websites, it is a "pen register" for the purposes of CIPA § 638.50(b).

2. ADNXS Tracker

[29] The last seven digits of Plaintiff's IP address have redacted for the purposes of this public filing to protect his privacy.

69. Microsoft is a technology company with software-as-a-service products, such as Microsoft Advertising. Microsoft owns and operates the ADNXS Tracker, which it provides to website owners like Defendant for a fee. Microsoft rebranded ADNXS to "Microsoft Invest," but the two are the same service. ADNXS is a DSP, as described below.

70. According to Microsoft, "[w]ith an integrated platform advantage and a focus on data-driven performance, [Microsoft] enables you to engage audiences on all screens and drive business results."[30]

71. In other words, Microsoft facilities the selling of Defendant's Website users to interested advertisers, who will bid to show those users advertisements targeted to their identity and location. This process enables Defendant to monetize its Website. To achieve this, Microsoft uses its Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Website.

72. The first time a user visits Defendant's Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends an HTTP response with directions to install the ADNXS Tracker on the user's browser. The ADNXS Tracker, in turn, instructs the user's browser to send Microsoft the user's IP address and Device Fingerprints.

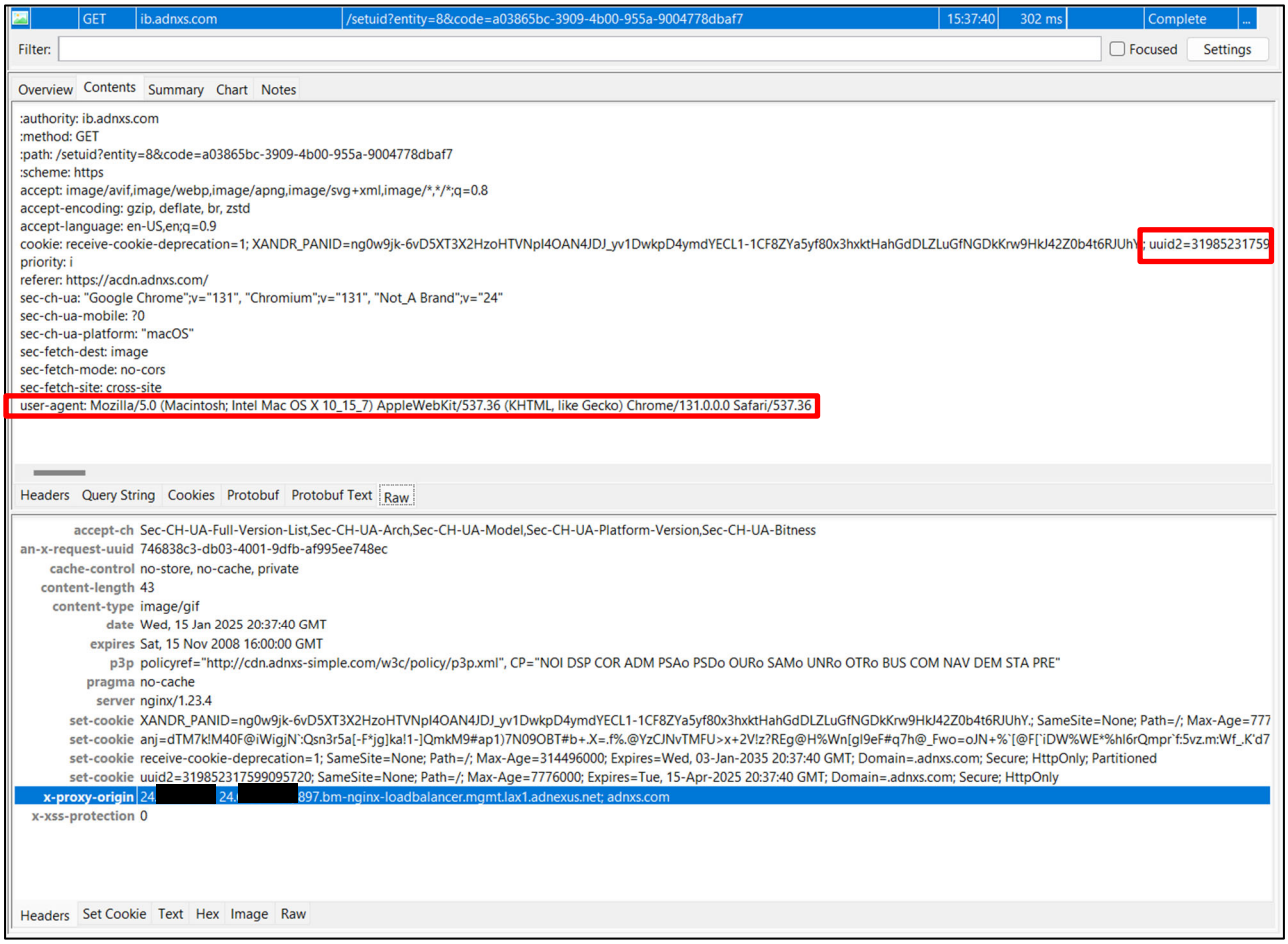
73. Moreover, Microsoft stores a cookie (the "UUID") with the user's IP address and Device Fingerprints in the user's browser cache. When the user subsequently visits Defendant's Website, the ADNXS Tracker locates the cookie identifier stored on the user's browser. If the cookie is stored on the browser, the ADNXS Tracker causes the browser to send the cookie along with the user's IP address and Device Fingerprints to Microsoft. A general diagram of this process is pictured as Figure 2, which explains how the Website causes the ADNXS Tracker to install a cookie on the user's browser and instructs the user's browser to send the user's IP address and Device Fingerprints along with the cookie.

[30] *Microsoft Invest*, MICROSOFT ADVERTISING, https://about.ads.microsoft.com/en/solutions/technology/microsoft-invest-dsp#accordionb751e6297a-item-73282c0a03 (last visited Dec. 23, 2024).

74. If the user clears his or her cookies, then the user wipes out the ADNXS Tracker from its cache. Accordingly, the next time the user visits Defendant's Website the process begins over again: (i) Defendant's server installs the ADNXS Tracker on the user's browser, (ii) the ADNXS Tracker instructs the browser to send Microsoft the user's IP address and Device Fingerprints, (iii) the ADNXS Tracker stores a cookie in the browser cache, and (iv) Microsoft will continue to receive the user's IP address and Device Fingerprints on subsequent Website visits as part of the cookie transmission.

75. In all cases, however, Microsoft receives a user's IP address, Device Fingerprints, and user information each and every time its Tracker is loaded by the Website, as the below screenshot indicates.

Figure 6:



76. The ADNXS Tracker is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, 684 F. Supp. 3d at 1050.

77. Further, the ADNXS Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *James*, 701 F. Supp. 3d at 958.

78. Because the ADNXS Tracker captures the outgoing information—the IP address—from visitors to websites, it is a "pen register" for the purposes of CIPA § 638.50(b).

3. OpenX Tracker

79. OpenX is a software-as-a-service company that develops and operates the OpenX Tracker, called" OpenAudience," which it provides to website owners like Defendant for a fee.

80. OpenX is a registered data broker in California[31] that develops, a "tool to help [companies, like Defendant,] utilize their [first party] data, leverage [third party data], and package up audiences for marketers that will drive ad revenue."[32]

81. OpenX takes this data and uses it to "match [a company's] audience against [OpenX's] graph to put users in audience segments that [OpenX] mak[es] available to marketers."[33]

82. In other words, OpenX compiles comprehensive user profiles by tracking users across the Internet. OpenX then enriches the information of its client's end users (like Defendant's end users) with the profile data to make that information more valuable to advertisers by aggregating that information into a graph, thereby driving Defendant's revenue. To achieve this, OpenX uses its OpenAudience Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant's Website.

83. The first time a user visits Defendant's Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends an HTTP response with directions to

[31] DATA BROKER REGISTRATION FOR OPENX TECHNOLOGIES, INC., https://oag.ca.gov/data-broker/registration/193614.

[32] *OpenAudience*, OPENX, https://www.openx.com/why-openx/openaudience/ (last accessed Jan. 27, 2025).

[33] *Data Activation*, OPENX, https://www.openx.com/why-openx/openaudience/ (last accessed Feb. 3, 2025).

install the OpenX Tracker on the user's browser. The OpenX Tracker, in turn, instructs the user's browser to send OpenX the user's IP address and Device Fingerprints.

84. Moreover, OpenX stores a cookie (the "univ_id" string below) with the user's IP address and Device Fingerprints in the user's browser cache. When the user subsequently visits Defendant's Website, the OpenX Tracker locates the cookie identifier stored on the user's browser. If the cookie is stored on the browser, the OpenX Tracker causes the browser to send the cookie along with the user's IP address and Device Fingerprints to OpenX. A general diagram of this process is pictured as Figure 2, which explains how the Website causes the OpenX Tracker to install a cookie on the user's browser and instructs the user's browser to send the user's IP address and Device Fingerprints through the cookie.

85. If the user clears his or her cookies, then the user wipes out the OpenX Tracker from its cache. Accordingly, the next time the user visits Defendant's Website the process begins over again: (i) Defendant's server installs the OpenX Tracker on the user's browser, (ii) the OpenX Tracker instructs the browser to send OpenX the user's IP address and Device Fingerprints, (iii) the OpenX Tracker stores a cookie in the browser cache, and (iv) OpenX will continue to receive the user's IP address and Device Fingerprints on subsequent Website visits as part of the cookie transmission.

86. In all cases, however, OpenX receives a user's IP address, Device Fingerprints, and user information each and every time its Tracker is loaded by the Website, as the below screenshot indicates:

//

//

//

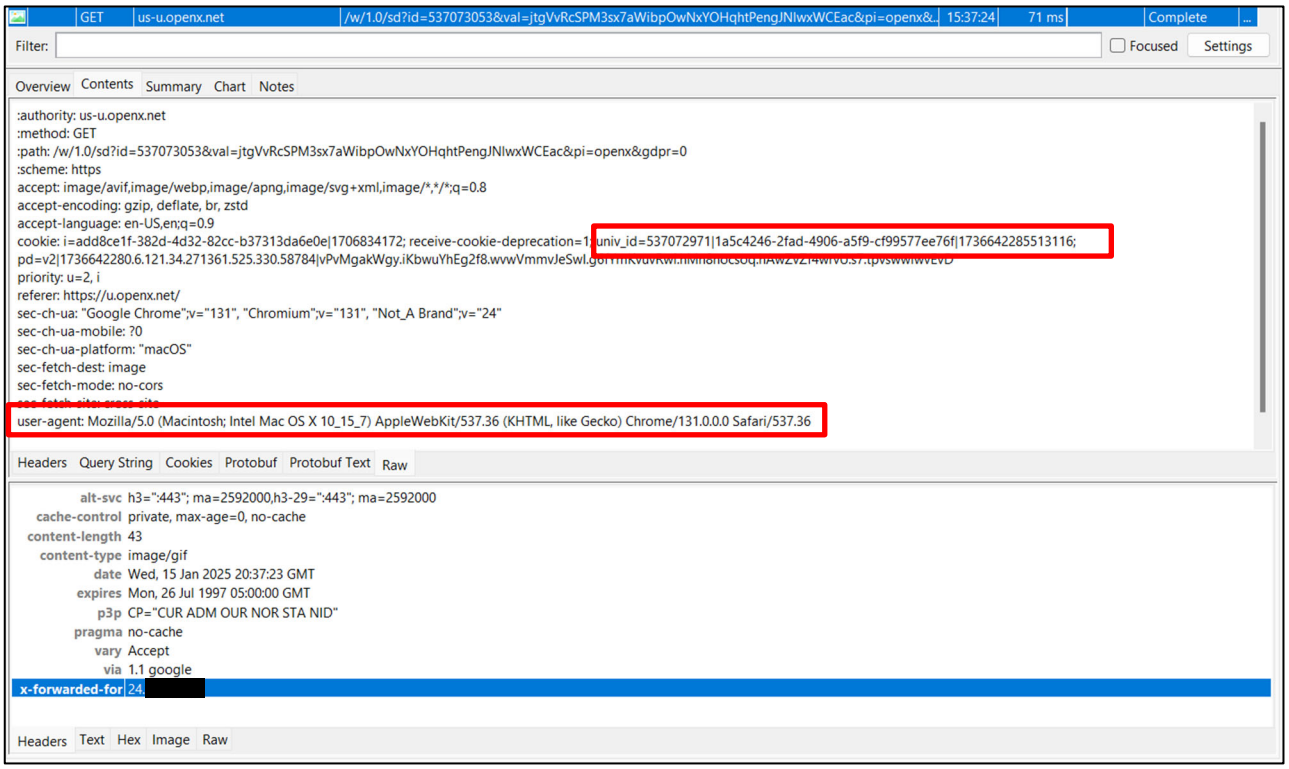
//

//

//

//

Figure 7:



87. The OpenX Tracker is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, 684 F. Supp. 3d at 1050.

88. Further, the OpenX Tracker is a "device" because "in order for software to work, it must be run on some kind of computing device." *James*, 701 F. Supp. 3d at 958.

89. Because the OpenX Tracker captures the outgoing information—the IP address—from visitors to websites, it is a "pen register" for the purposes of CIPA § 638.50(b).

III. DEFENDANT'S CONDUCT CONSTITUTES AN INVASION OF PLAINTIFF'S AND CLASS MEMBERS' PRIVACY

90. The collection of Plaintiff's and Class Members' personally identifying, non-anonymized information through Defendant's installation and use of the Trackers constitutes an invasion of privacy.

91. As alleged herein, the Trackers are designed to conduct targeted advertising and boost Defendant's revenue, all through their surreptitious collection of Plaintiff's and Class Members' personal information.

A. Data Brokers and Real-Time Bidding: The Information Economy

92. To put the invasiveness of Defendant's violations of the CIPA into perspective, it is also important to understand two concepts: data brokers and real-time bidding.

1. Data Brokers

93. While "[t]here is no single, agreed-upon definition of data brokers in United States law,"[34] California law defines a "data broker" as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct [*i.e.*, consumer-facing] relationship," subject to certain exceptions. Cal. Civ. Code § 1798.99.80(c).

94. Any entity that qualifies as a "data broker" under California law must specifically register as such Cal. Civ. Code § 1798.99.82(a), which OpenX does.[35]

95. "Data brokers typically offer pre-packaged databases of information to potential buyers," either through the "outright s[ale of] data on individuals" or by "licens[ing] and otherwise shar[ing] the data with third parties."[36] Such databases are extensive, and can "not only include information publicly available [such as] from Facebook but also the user's exact residential address, date and year of birth, and political affiliation," in addition to "inferences [that] can be made from the combined data."[37]

96. For instance, the NATO report noted that data brokers collect two sets of information: "observed and inferred (or modelled)." The former "is data that has been collected and is actual," such as websites visited." Inferred data "is gleaned from observed data by modelling or profiling," meaning what users may be *expected* to do. On top of this, "[b]rokers typically collect not only what

[34] JUSTIN SHERMAN, DUKE SANFORD CYBER POLICY PROGRAM, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS: THREATS TO AMERICAN CIVIL RIGHTS, NATIONAL SECURITY, AND DEMOCRACY, 2 (DUKE SANFORD CYBER POLICY PROGRAM, 2021), https://tinyurl.com/hy9fewhs.

[35] DATA BROKER REGISTRATION FOR OPENX TECHNOLOGIES, INC., https://oag.ca.gov/data-broker/registration/193614.

[36] SHERMAN, *supra*, at 2.

[37] Tehila Minkus et al., *The City Privacy Attack: Combining Social Media and Public Records for Detailed Profiles of Adults and Children*, COSN '15: PROCEEDINGS OF THE 2015 ACM ON CONFERENCE ON ONLINE SOCIAL NETWORKS 71, 71 (2015), https://dl.acm.org/doi/pdf/10.1145/2817946.2817957.

they immediately need or can use, but hoover up as much information as possible to compile comprehensive data sets that might have some future use."[38]

97. Likewise, a report by the Duke Sanford Cyber Policy Program "examine[d] 10 major data brokers and the highly sensitive data they hold on U.S. individuals."[39] The report found that "data brokers are openly and explicitly advertising data for sale on U.S. individuals' sensitive demographic information, on U.S. individuals' political preferences and beliefs, on U.S. individuals' whereabouts and even real-time GPS locations, on current and former U.S. military personnel, and on current U.S. government employees."[40]

98. This data collection has grave implications for Americans' right to privacy. For instance, "U.S. federal agencies from the Federal Bureau of Investigation [] to U.S. Immigration and Customs Enforcement [] purchase data from data brokers—without warrants, public disclosures, or robust oversight—to carry out everything from criminal investigations to deportations."[41]

99. As another example:

> Data brokers also hold highly sensitive data on U.S. individuals such as race, ethnicity, gender, sexual orientation, immigration status, income level, and political preferences and beliefs (like support for the NAACP or National LGBTQ Task Force) that can be used to directly undermine individuals' civil rights. Even if data brokers do not explicitly advertise these types of data (though in many cases they do), everything from media reporting to testimony by a Federal Trade Commission commissioner has identified the risk that data brokers use their data sets to make "predictions" or "inferences" about this kind of sensitive information (race, gender, sexual orientation, etc.) on individuals.
>
> This data can be used by commercial entities within the U.S. to discriminately target goods and services, akin to how Facebook advertising tools allow advertisers to exclude certain groups, such as those who are identified as people with disabilities or those who are identified as Black or Latino, from seeing advertisements. 59 Many industries from health insurance to life insurance to banking to e-commerce purchase data from data brokers to run advertisements and target their services.

[38] TWETMAN & BERGMANIS-KORATS, *supra*, at 11.

[39] SHERMAN, *supra*, at 1.

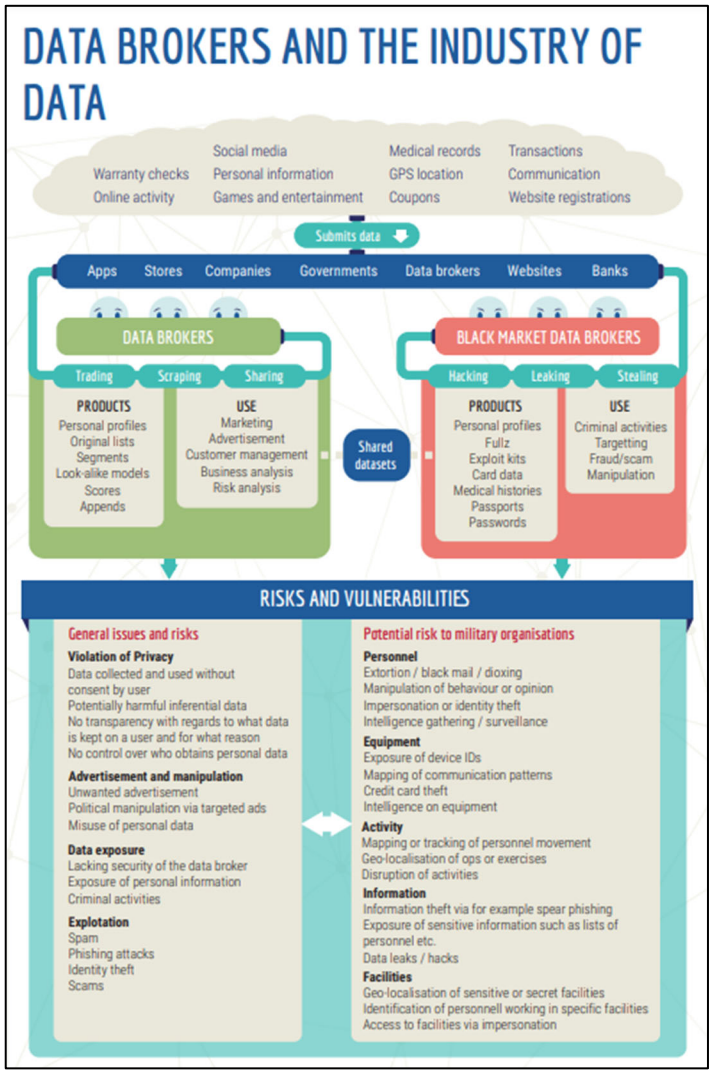
[40] *Id*.

[41] *Id.* at 9.

> …
>
> Given identified discrimination problems in machine learning algorithms, there is great risk of these predictive tools only further driving up costs of goods and services (from insurance to housing) for minority groups.[42]

100. Similarly, as the report from NATO noted, corporate data brokers cause numerous privacy harms, including but not limited to depriving users of the right to control who does and does not acquire their personal information, unwanted advertisements that can even go as far as manipulating viewpoints, and spam and phishing attacks.[43]

Figure 8:



[42] *Id.*

[43] TWETMAN & BERGMANIS-KORATS, *supra*, at 8.

101. As noted above, data brokers, like OpenX, are able to compile such wide swaths of information in part by collecting users' IP addresses and Device Fingerprints, which is used by data brokers, like OpenX, to track users across the Internet.[44] Indeed, as McAfee (a data security company) notes, "data brokers can … even place trackers or cookies on your browsers … [that] track your IP address and browsing history, which third parties can exploit."[45]

102. These data brokers will then:

> take that data and pair it with other data they've collected about you, pool it together with other data they've got on you, and then share all of it with businesses who want to market to you. They can eventually build large datasets about you with things like: "browsed gym shorts, vegan, living in Los Angeles, income between $65k-90k, traveler, and single." Then, they sort you into groups of other people like you, so they can sell those lists of like-people and generate their income.[46]

103. In short, by collecting IP addresses and Device Fingerprints, data brokers, like OpenX, can track users across the Internet, compiling various bits of information about users, building comprehensive user profiles that include an assortment of information, interests, and inferences, and offering up that information for sale to the highest bidder. The "highest bidder" is a literal term, as explained below.

104. As a result of Defendant's installation the trackers of data brokers, like OpenX, on the browsers of users of Defendant's Website, the information of Plaintiff and Class Members is linked to any profiles these data brokers may have about them using their IP addresses and Device Fingerprints (or new profiles are created for Plaintiff and Class Members). These profiles are then served up to any companies that want to advertise on Defendant's Website, and Defendant's users become more valuable as a result of having their IP addresses and Device Fingerprint Information linked to these data broker profiles. Thus, Defendant is unjustly enriched through advertising revenue by installing the Trackers on Plaintiff's and Class Members' browsers, and thus, enabling

---

[44] *Id.* at 11.

[45] Jasdev Dhaliwal, *How Data Brokers Sell Your Identity*, MCAFEE (June 4, 2024), https://www.mcafee.com/blogs/tips-tricks/how-data-brokers-sell-your-identity/.

[46] Paul Jarvis, *The Problem with Data Brokers: Targeted Ads and Your Privacy*, FATHOM ANALYTICS (May 10, 2022), https://usefathom.com/blog/data-brokers.

the Third Parties to collect Plaintiff's and Class Members' IP addresses and Device Fingerprints without consent.

2. Real-Time Bidding

105. So, once data brokers like OpenX collect Website users' IP addresses and Device Fingerprints and create or link that information to comprehensive user profiles, how does OpenX "sell" or otherwise help Defendant monetize that information? This is where real-time bidding—and Microsoft's ADNXS Tracker and the Connatix's Tracker—comes in.

106. "Real Time Bidding (RTB) is an online advertising auction that uses sensitive personal information to facilitate the process to determine which digital ad will be displayed to a user on a given website or application."[47]

107. "There are three types of platforms involved in an RTB auction: Supply Side Platforms (SSPs), Advertising Exchanges, and Demand Side Platforms (DSPs)." An SSP, which is what the Connatix Tracker is, "work[s] with website or app publishers to help them participate in the RTB process." "DSPs [which is what the ADNXS Tracker is[48]] primarily work with advertisers to help them evaluate the value of user impressions and optimize the bid prices they put forth."[49] And an Advertising Exchange—which both Connatix[50] and Microsoft[51] provide—"allows advertisers and publishers to use the same technological platform, services, and methods, and "speak the same language" in order to exchange data, set prices, and ultimately serve an ad."[52]

---

[47] Sara Geoghegan, *What is Real Time Bidding?*, ELECTRONIC PRIVACY INFORMATION CENTER (Jan. 15, 2025), https://epic.org/what-is-real-time-bidding/.

[48] MICROSOFT INVEST, https://about.ads.microsoft.com/en/solutions/technology/microsoft-invest-dsp ("Microsoft Invest is a demand-side platform built for the future of video advertising.").

[49] Geoghegan, *supra*.

[50] CONNATIX, VIDEO MONETIZATION, https://connatix.com/video-monetization ("Powered by an integrated ad server and exchange, access premium demand while growing direct sales efforts.").

[51] ABOUT MICROSOFT INVEST, MICROSOFT IGNITE (Feb. 12, 2024), https://learn.microsoft.com/en-us/xandr/invest/about-invest ("The Microsoft Advertising platform is a real-time bidding system and ad server.").

[52] *Introducing To Ad Serving*, MICROSOFT IGNITE (Mar. 3, 2024), https://learn.microsoft.com/en-us/xandr/industry-reference/introduction-to-ad-serving.

108. In other words, SSPs like the Connatix Tracker provide user information to advertisers that might be interested in those users, DSPs like the ADNXS Tracker help advertisers select which users to advertise and target, and an Advertising Exchange is the platform on which all of this happens.

109. The RTB process works as follows:

> After a user loads a website or app, an SSP will send user data to Advertising Exchanges … The user data, often referred to as "bidstream data," contains information like device identifiers, IP address, zip/postal code, GPS location, browsing history, location data, and more. After receiving the bidstream data, an Advertising Exchange will broadcast the data to several DSPs [here, Microsoft]. The DSPs will then examine the broadcasted data to determine whether to make a bid on behalf of their client.
>
> Ultimately, if the DSP wins the bid, its client's advertisement will appear to the user. Since most RTB auctions are held on the server/exchange side, instead of the client/browser side, the user only actually sees the winner of the auction and would not be aware of the DSPs who bid and lost. But even the losing DSPs still benefit because they also receive and collect the user data broadcasted during the RTB auction process. This information can be added to existing dossiers DSPs have on a user.[53]

Figure 9:

[53] Geoghegan, *supra*; *see also* REAL-TIME BIDDING, APPSFLYER, https://www.appsflyer.com/glossary/real-time-bidding/.

110. Facilitating this real-time bidding process means a DSP like Microsoft must have as much information as possible about Defendant's users to procure the greatest interest from advertisers and the highest bids. But Microsoft receives assistance because Defendant also installs OpenX's Tracker on its users' browsers:

> the economic incentives of an auction mean that DSP with more specific knowledge of individuals will win desirable viewers due to being able to target them more specifically and out-bid other entities. As a consequence, the bid request is not the end of the road. The DSP enlists a final actor, the data management platform (DMP). DSPs send bid requests to DMPs, who enrich them by attempting to identify the user in the request and use a variety of data sources, such as those uploaded by the advertiser, collected from other sources, or bought from data brokers [here, OpenX]. The DSP with the highest bid not only wins the right to deliver the ad—through the SSP—to the individual. The DSP also wins the right to cookie sync its own cookies with those from the [Advertising Exchange, here, Connatix], thus enabling easier linkage of the data to the user's profile in the future.[54]

111. In other words, before bidding to show a user an advertisement, a DSP will attempt to determine what other information about a user may be available. A DSP does this by connecting with an entity like OpenX, whose Tracker matches the IP address and Device Fingerprints it collects from Website users (as well as the cookie it sets on the user's browser) with any profiles on those users OpenX may have compiled. If there is a match, then advertisers will pay more money to show users an advertisement because the advertisers have more information to base their targeting on. This naturally enriches Defendant, as its users have now become more valuable. And, a DSP like Microsoft is able to continue linking users on Defendant's Website through the Advertising Exchange, which enhances Microsoft's ability to better identify Defendant's users in the future.

112. As the Federal Trade Commission ("FTC") has noted, "[t]he use of real-time bidding presents potential concerns," including but not limited to:

> (a) "incentiviz[ing] invasive data-sharing" by "push[ing] publishers [*i.e.*, Defendant] to share as much end-user data as possible to get higher valuation for their ad inventory—particularly their location data and cookie cache, which can be used to ascertain a person's browsing history and behavior."

[54] Michael Veale & Federik Zuiderveen Borgesius, *Adtech and Real-Time Bidding under European Data Protection Law*, 23 GERMAN L. J. 226, 232-33 (2022) https://tinyurl.com/yjddt5ey.

(b) "send[ing] sensitive data across geographic borders."

(c) sending consumer data "to potentially dozens of bidders simultaneously, despite only one of those parties—the winning bidder actually using that data to serve a targeted ad. Experts have previously cautioned that there are few (if any) technical controls ensuring those other parties do not retain that data for use in unintended ways."[55]

113. Given Microsoft operates a DSP here, the last point is particularly relevant, as it means Microsoft—through the ADNXS Tracker—collects and discloses Website users' information to *all prospective advertisers*, even if advertisers do not ultimately show a user an advertisement. This greatly diminishes the ability of users to control their personal information.

114. Likewise, the Electronic Privacy Information Center ("EPIC") has warned that "[c]onsumers' privacy is violated when entities disclose their information without authorization or in ways that thwart their expectations."[56]

115. All of this is in line with protecting the right to determine who does and does not get to know one's information, a harm long recognized at common law and one the CIPA was enacted to protect against. *Ribas*, *supra*, 38 Cal. 3d at 361 (noting the CIPA was drafted with a two-party consent requirement to protect "the right to control the nature and extent of the firsthand dissemination of [one's] statements"); *Dep't of Justice v. Reporters Comm. for Freedom of the Press* 489 U.S. 749, 763-64 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.").

* * *

116. To summarize the proceeding allegations, Defendant monetizes its Website (in part) by installing the Connatix and ADNXS Trackers on its users' browsers, and therefore enabling Connatix and Microsoft to collect Website users' IP addresses and Device Fingerprints. Microsoft then provides that information to advertisers who are interested in showing advertisements to Website users, and Microsoft provides the bids of these advertisements to Defendant through the

[55] FEDERAL TRADE COMMISSION, UNPACKING REAL TIME BIDDING THROUGH FTC'S CASE ON MOBILEWALLA (Dec. 3, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla.

[56] Geoghegan, *supra*.

real-time bidding process. Connatix likewise offers up Defendant's users for sale to advertisers on the Advertising Exchange, and thus collects this information from users as well when Defendant installs the Connatix Tracker on browsers. The winning bidder ultimately has their advertisement displayed to Website users, but all interested advertisers receive Website users' information regardless.

117. The value of those users is enriched because Defendant also installs the OpenX Tracker on Website users' browsers, which enables OpenX to collect Website users' IP addresses and Device Fingerprints. OpenX then matches that information to profiles it maintains on those users and supplies advertisers with that information to better inform advertisers' bids. This causes advertisers to bid more money to show an advertisement to Defendant's users because advertisers are better able to target their advertising by knowing more about Defendant's users.

118. Thus, Defendant is unjustly enriched through its installation and use of the Trackers, which causes data to be collected by Third Parties without Plaintiff's and Class Members' consent, and which enable the Third Parties to sell Defendant's user inventory in an ad-buying system. In addition, Plaintiff and Class Members lose the ability to control their information, as their information ends up in the hands of data brokers, advertising inventory sellers, and advertisers themselves without knowledge or consent. And, because Defendant installs the OpenX Tracker on Plaintiff's and Class Members' browsers, OpenX continues to track Plaintiff and Class Members wherever they go online, this building even more comprehensive user profiles over time that are provider to OpenX's other clients (or further enrich Defendant here).

B. Defendant Uses The Connatix Tracker For Targeted Advertising And Data Monetization

119. Connatix is "the industry's most comprehensive independent video technology and monetization platform for broadcasters, publishers, and advertisers" and "currently works with 350+ publisher groups across thousands of sites" to "help[] publishers deliver, monetize, analyze and create video."[57]

[57] *Connatix and JW Player Merge To Create the Industry's Largest Video Technology and Monetization Platform*, PR NEWSWIRE (Oct. 9, 2024), https://www.prnewswire.com/news-

120. Connatix offers a number of solutions to help companies like Defendant market, advertise, and analyze user data from its website, "leveraging insights from content and audiences to help maximize revenue."[58] For example, Connatix enables publishers to place advertisements on their webpages, social media, or in videos.

121. Connatix's solutions include "Video Monetization," which allows its clients, like Defendant, to "access premium demand while growing direct sales efforts" "powered by an integrated ad server and exchange"[59] and "Video Analytics," which enables its clients, like Defendant, to "[e]asily access analytics with extensive reporting tools" and "[g]et on-demand analytics" for, among other things, "[a]dvertising performance."[60]

122. Importantly "Connatix's suite [also] includes a[n] … ad server, SSP and [sic] contextual ad platform."[61] This means that Connatix gathers the IP address and Device Fingerprints of Defendant's website users and then connects Defendant with DSPs, like ADNXS, to sell customer's information.

123. Connatix proudly touts that it provides these services to "publishers like … BuzzFeed" (Defendant's parent company) to "increase revenue from video media).[62]

124. Connatix also helps advertisers "[a]mplify campaign performance," "[i]ncrease efficiency," and "[d]eliver at scale against premium video inventory when readers are immersed" in "editorial content or story-like formats."[63]

releases/connatix-and-jw-player-merge-to-create-the-industrys-largest-video-technology-and-monetization-platform-302271377.html (last visited Dec. 23, 2024).

[58] *Id.*

[59] *Video Monetization*, CONNATIX, https://connatix.com/video-monetization (last visited Dec. 23, 2024).

[60] *Video Analytics*, CONNATIX, https://connatix.com/video-analytics (last visited Dec. 23, 2024).

[61] *Connatix – Helping Publishers Create, Host and Monetize Video Assets*, CONNATIX (Aug. 9, 2022), https://connatix.com/press/connatix-helping-publishers-create-host-and-monetize-video-assets.

[62] CONNATIX – HELPING PUBLISHERS CREATE, HOST AND MONETIZE VIDEO ASSETS, https://www.youtube.com/watch?v=-w-bxrcsrt0.

[63] *Advertisers*, CONNATIX, https://connatix.com/advertisers (last visited Dec. 23, 2024).

125. Connatix "collect[s] and process[es]" "through a cookie saved on the device you use to access the internet" "some of [the following] information": "[a] unique user ID that Connatix generates and is fetched when you access various publisher sites," "[t]he IP address of the device you use to access the Internet," "[y]our approximate (city-granular) location derived from IP address," and the "browser type, language, and operating system you use."[64] Connatix further explains "[w]e use the information explained above for a number of purposes" including "[t]o show you ads based on the content you're viewing, the app you're using, your approximate location, and your device type" and "[t]o show you personalized ads and other content based on a profile about your visits to Online Properties and your approximate location."[65]

126. To perform the functions listed above, Connatix needs to collect data that identifies a particular user. This is why Connatix collects IP addresses: it allows Connatix to ascertain a user's identity and target that user with personalized advertisements, as well as to track a user's Website activity over time (*i.e.*, through repeated Website visits) to target a user with advertisements relevant to the user's personal browsing activity.

127. Further, because the Connatix Tracker is present on multiple websites, Connatix is able to track Plaintiff and Class Members across multiple websites using their IP addresses and other device identifier information, and build a more complete profile of Plaintiff and Class Members for advertising purposes (including to assist Defendant's advertising) using this same information.

C. Defendant Uses The ADNXS Tracker For Targeted Advertising And Data Monetization

128. Microsoft describes its advertising services, which include the ADNXS or Microsoft Invest Tracker, as "a strategic buying platform built for the needs of today's advertisers looking to invest in upper-funnel buying and drive business results."[66]

[64] *See* GENERAL PRIVACY, CONNATIX, https://connatix.com/privacy-policy (last visited Dec. 22, 2024).

[65] *Id.*

[66] *About Microsoft Invest*, MICROSOFT IGNITE (Feb. 12, 2024), https://learn.microsoft.com/en-us/xandr/invest/about-invest (last visited Dec. 23, 2024).

129. Microsoft collects data to help companies with their marketing; when the processing system "receives ad requests, [it] applies data to the request, receives bids, makes decisions, serves creatives, logs, auctions, etc."[67]

130. In particular:

> The Microsoft Advertising platform is a real-time bidding system and ad server. The main processing system is called the "impression bus." The impression bus receives ad requests, applies data to the request, receives bids, makes decisions, serves creatives, logs auctions, etc.
>
> Ad calls come in via our inventory supply partners: exchanges, SSPs, ad networks, and a few valued publishers.
>
> …
>
> Once we get the call, we overlay segment data from our server-side cookie store. Data is added to the cookie store either through Xandr segment pixels or by clients sending us a file of data. We also contact third-party data providers and overlay any available data.
>
> We contact all of the bidders on our platform. The ad call includes whatever user data belongs to each bidder, and information about the inventory. Bidders have a certain number of milliseconds in which to respond with a bid and the creative they want to serve.
>
> …
>
> The impression bus decides which bid wins based on the amount of the bid, and any preferences the publisher has about what they want served on their page. If the call was client-side, Microsoft Advertising serves the ad. If it was server-side, Microsoft Advertising passes the bid and the location of the creative to the partner who will ultimately serve the ad. [68]

131. Microsoft Invest (*i.e.*, the ADNXS Tracker) provides "targeting, bidding algorithms, multi-currency support, and all the other features of a premium ad server."[69] To do this, Microsoft utilizes data from its cookie store. The "[d]ata is added to the cookie store either through Microsoft Advertising segment pixels or by clients sending [them] a file of data. [They] also contact third-party data providers and overlay any available data."[70]

---

[67] *Id.*

[68] https://learn.microsoft.com/en-us/xandr/invest/about-invest

[69] *About Microsoft Invest*, MICROSOFT IGNITE (Feb. 12, 2024), https://learn.microsoft.com/en-us/xandr/invest/about-invest

[70] *Id.*

132. Microsoft also integrates with the OpenX Tracker on Defendant's Website to enrich Defendant's user data and therefore obtain higher bids to show advertisements to Defendant's users. And Microsoft discloses all of this information to advertisers that bid on Defendant's users, regardless of whether the advertiser actually wins the bid.

133. Further, Microsoft utilizes data from its cookie store. The "[d]ata is added to the cookie store either through Microsoft Advertising segment pixels or by clients sending [them] a file of data. [They] also contact third-party data providers and overlay any available data."[71]

134. In other words, when users visit Defendant's Website, Microsoft collects users' IP addresses and Device Fingerprints through its ADNXS Tracker to provide to advertisers interested in showing an advertisement to Defendant's Website users, enriching that information by integrating with the OpenX Tracker (and its own data), and ultimately enabling Defendant to monetize its Website and maximize revenue by collecting and disclosing user information.

D. Defendant Uses The OpenX Tracker For Identity Resolution, Targeted Advertising, And Data Monetization

135. As noted above, OpenX is a registered Data Broker in California that claims to be "the world's leading independent supply-side platform for audience, data, and identity targeting."[72]

136. OpenX's "proprietary identity resolution tool, OpenAudience, uses state-of-the-art data and identity technology to allow marketers to reach their target audiences and segments — connecting [companies] to [their] desired consumers in more ways than you have ever imagined possible."[73]

137. OpenX does this by taking a company's "first-party data, or any pre-built audience segments, and seamlessly match[ing it] to [OpenX's] identity graph of more than 200 million unique people."[74]

[71] *Id.*

[72] *About Us*, OPENX, https://www.openx.com/company/ (last accessed Jan. 27, 2025).

[73] *Buyers*, OPENX, https://www.openx.com/company/ (last accessed Jan. 27, 2025).

[74] *OpenAudience*, OPENX, https://www.openx.com/company/ (last accessed Jan. 27, 2025).

138. In other words, OpenAudience gathers information of Defendant's website users, such as IP addresses and Device Fingerprints, compares it against their own records, and combines the two to enhance the information into a deanonymized profile of each individual website visitor.

139. OpenX can then use these individual profiles to provide marketers, such as Defendant, with curated packages that identify and target specific customers.[75]

140. OpenX splits this up into two different types of packages. The first are inventory packages that allows marketers to "[s]howcase [their] brand alongside brand-safe inventory across [OpenX's] network of trusted publishers, reaching consumers *wherever* and *whenever* they engage with their favorite content."[76] The second are data driven packages that "[e]ngage customers with packages powered by data-driven curation, and drive performance on brand-safe inventory. [Allowing companies, like Defendant to e]ffortlessly choose from pre-built packages powered by audience, contextual, attention, or sustainability data and [OpenX's] proprietary identity graph."[77]

141. This identity graph provides companies, like Defendant and the other Third Parties, access to 800 million hashed emails, 200 million hashed phone numbers, over 200 million U.S. users instrumented for data and identity, 48 million CTV users instrumented for data and identity, over 5,000 requests per user per month, and 3,000 data attributes available for targeting.[78]

142. In other words, OpenX utilizes third-party data (*i.e.*, data OpenX collects on its own), as well as data from the publisher where the ad is ultimately placed (*i.e.*, first-party, like data directly from Defendant's Website users), to determine where to place advertisers' ads and who to place them in front of.

[75] *Curated Packages*, OPENX, https://www.openx.com/curated-packages/ (last accessed Feb. 4, 2025).

[76] *Id.* (emphasis added).

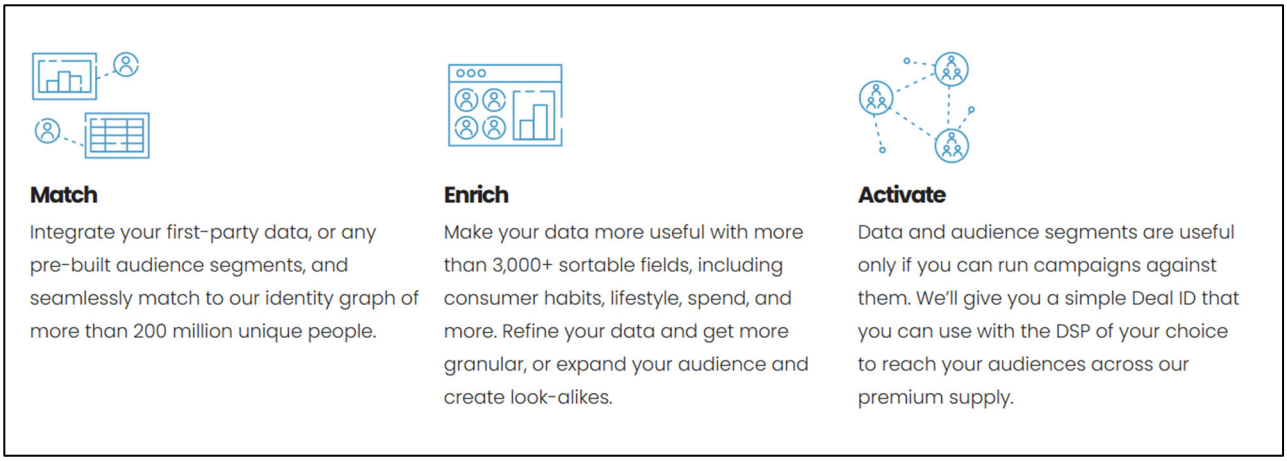
[77] *Id.*

[78] *OpenAudience*, OPENX, https://www.openx.com/company/ (last accessed Jan. 27, 2025).

143. By way of example, OpenX sells a "Health Insurance Data Driven Package" that targets consumers who have viewed advertisements from health insurance advertisers.[79] As such, this helps companies target people who have indicated an interest in specific health insurance related content.

144. To do all of this, OpenX needs to collect data that identifies a particular user. This is why OpenX collects IP addresses and Device Fingerprints: it allows OpenX to link one of Defendant's Website users to any profile OpenX may have about that user, and OpenX can in turn provide that profile to interested advertisers for more targeted advertising. The IP address, Device Fingerprints, and OpenX cookie, also allow OpenX to track a user's Website activity over time (*i.e.*, through repeated Website visits) and to track that user on other websites.

Figure 10:



145. In other words, when users visit Defendant's Website, OpenX collects users' IP addresses through its OpenAudience Tracker to build comprehensive user profiles, which are used to identify Defendant's users, enrich Defendant's user data, and make those users more valuable to prospective advertisers by allowing advertisers to better target specific users. All of this helps Defendant further monetize its Website and maximize revenue by collecting and disclosing user information.

[79] *Health Insurance Data Driven Package*, OPENX, https://www.openx.com/curated-packages/health-insurance/ (last accessed Feb. 04, 2025).

IV. PLAINTIFF'S EXPERIENCE

146. Plaintiff regularly visits the Website on his desktop browser—as long ago as 2018 and as recently as January 13, 2025—and has done so throughout the entirety of the class period.

147. When Plaintiff visited the Website, the Website's code—as programmed by Defendant—caused the Connatix Tracker to be installed on Plaintiff's browser. This allowed Connatix, through its Tracker, to collect Plaintiff's IP address, Connatix ID (8c9a4fb0a60e4386b0b3ee02ec13beb1), browser, operating system, and device type (Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36). *See* Figure 5, *supra*.

148. When Plaintiff visited the Website, the Website's code—as programmed by Defendant—caused the ADNXS Tracker to be installed on Plaintiff's browser. This allowed Microsoft, through its Tracker, to collect Plaintiff's IP address, UUID (31985231759), browser, operating system, and device type (Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36). *See* Figure 6.

149. When Plaintiff visited the Website, the Website's code—as programmed by Defendant—caused the OpenX Tracker to be installed on Plaintiff's browser. This allowed OpenX, through its Tracker, to collect Plaintiff's IP address, OpenX ID (537072971|1a5c4246-2fad-4906-a5f9-cf99577ee76f|1736642285513116), browser, operating system, and device type (Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36). *See* Figure 7.

150. Defendant and the Third Parties used the information collected by the Trackers to identity Plaintiff and either create a new profile of him in OpenX's database or match Plaintiff to a pre-existing profile, provide Plaintiff's information to advertisers for hyper-targeted advertising based (in part) on Plaintiff's location, and ultimately boost Defendant's and advertisers' revenue.

151. Plaintiff did not provide his prior consent to Defendant to install or use the Trackers on Plaintiff's browser.

152. Defendant did not obtain a court order before installing or using the Trackers.

153. Plaintiff has had his privacy invaded by Defendant's violations of CIPA § 638.51(a).

154. Although Defendant utilizes at least three different Trackers on the Website (Connatix, ADNXS, and OpenX), they all operate in the same manner and perform the same function, *i.e.*, collecting Plaintiff's and Class members' IP addresses. Thus, at any given time a user visits the Website, Defendant will cause one of the Trackers to be installed on users' browsers for the purpose of collecting IP addresses.

155. Plaintiff and Class Members did not provide their prior consent to Defendant to install or use the Trackers on their browsers.

156. Defendant did not obtain a court order before installing or using the Trackers.

157. Thus, like Plaintiff, Class Members have also had their privacy invaded by Defendant's violations of CIPA § 638.51(a).

CLASS ALLEGATIONS

158. Pursuant to Fed. R. Civ. P. Rule 23(a) and 23(b)(3), Plaintiff seeks to represent a class defined as all California residents who accessed the Website in California and had their IP address collected by the Trackers (the "Class").

159. The following people are excluded from the Class: (i) any Judge presiding over this action and members of her or her family; (ii) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or their parents have a controlling interest (including current and former employees, officers, or directors); (iii) persons who properly execute and file a timely request for exclusion from the Class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) Plaintiff's counsel and Defendant's counsel; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

160. **Numerosity:** The number of people within the Class is substantial and believed to amount to thousands, if not millions of persons. It is, therefore, impractical to join each member of the Class as a named plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the

merits of this litigation. Moreover, the Class is ascertainable and identifiable from Defendant's records.

161. **Commonality and Predominance:** There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary between members of the Class, and which may be determined without reference to the individual circumstances of any Class Member, include, but are not limited to, the following:

(a) Whether Defendant violated CIPA section 638.51(a);

(b) Whether the Trackers are "pen registers" pursuant to Cal. Penal Code § 638.50(b);

(c) Whether Defendant sought or obtained prior consent—express or otherwise—from Plaintiff and the Class;

(d) Whether Defendant sought or obtained a court order for its use of the Trackers; and

(e) Whether Plaintiff and members of the Class are entitled to actual and/or statutory damages for the aforementioned violations.

162. **Typicality:** The claims of the named Plaintiff are typical of the claims of the Class because the named Plaintiff, like all other members of the Class Members, visited the Website and had his IP address collected by the Trackers, which were installed and used by Defendant.

163. **Adequate Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class Members he seeks to represent, he has retained competent counsel experienced in prosecuting class actions, and he intends to prosecute this action vigorously. The interests of members of the Class will be fairly and adequately protected by Plaintiff and his counsel.

164. **Superiority:** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of members of the Class. Each individual member of the Class may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial

system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSES OF ACTION

COUNT I
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 638.51(a)

165. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

166. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

167. CIPA section 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

168. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

169. The Trackers are "pen registers" because they are "device[s] or process[es]" that "capture[d]" the "routing, addressing, or signaling information"—the IP address—from the electronic communications transmitted by Plaintiff's and the Class's computers or smartphones. Cal. Penal Code § 638.50(b).

170. At all relevant times, Defendant installed the Trackers—which are pen registers—on Plaintiff's and Class Members' browsers, and used the Trackers to collect Plaintiff's and Class Members' IP addresses.

171. The Trackers do not collect the content of Plaintiff's and the Class's electronic communications with the Website. *In re Zynga Privacy Litig.,* 750 F.3d 1098, 1108 (9th Cir. 2014) ("IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication…") (cleaned up) .

172. Plaintiff and Class Members did not provide their prior consent to Defendant's installation or use of the Trackers.

173. Defendant did not obtain a court order to install or use the Trackers.

174. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by Defendant's violations of CIPA § 638.51(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 638.51(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order certifying the Class, naming Plaintiff as the representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order declaring that Defendant's conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For statutory damages of $5,000 for each violation of CIPA § 638.51(a);

(e) For pre- and post-judgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of equitable monetary relief; and

(g) For an order awarding and the Class their reasonable attorney's fees and expenses and costs of suit.

JURY DEMAND

Plaintiff demands a trial by jury on all causes of action and issues so triable.

Dated: February 13, 2025

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Emily A. Horne*
Emily A. Horne

L. Timothy Fisher (State Bar No. 191626)
Emily A. Horne (State Bar No. 347723)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
ehorne@bursor.com

Attorneys for Plaintiff